REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
	Technical Report	-

4. TITLE AND SUBTITLE
Ultra-Dense Quantum Communication Using Integrated Photonic Architecture: Second Quarterly Report

5a. CONTRACT NUMBER
W911NF-10-1-0416

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
0D10BH

6. AUTHORS
Dirk Englund, Karl Berggren, Seth Lloyd, Jeffrey Shapiro, Chee Wei Wong, Franco Wong, and Gregory Wornell

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Columbia University
615 West 131st Street, Room 254, Mail Code 8725
Studebaker Building
New York, NY 10027 -7922

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
58496-PH-DRP.2

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
We report on progress towards the goal of establishing a fundamental information-theoretic un- derstanding of quantum secure communication and devising practical and scalable implementations of quantum key distribution protocols in a photonic integrated chip platform.

15. SUBJECT TERMS
quantum information; quantum key distribution; secure communication; photonics; photonic networks; photonic interconnects

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dirk Englund
UU	UU	UU	UU		19b. TELEPHONE NUMBER 212-851-5958

Report Title

Ultra-Dense Quantum Communication Using Integrated Photonic Architecture: Second Quarterly Report

ABSTRACT

We report on progress towards the goal of establishing a fundamental information-theoretic un- derstanding of quantum secure communication and devising practical and scalable implementations of quantum key distribution protocols in a photonic integrated chip platform.

Ultra-Dense Quantum Communication Using Integrated Photonic Architecture
Second Quarterly Report

Dirk Englund, Karl Berggren, Seth Lloyd, Jeffrey Shapiro, Chee Wei Wong, Franco Wong, and Gregory Wornell
(Dated: April 30, 2011)

We report on progress towards the goal of establishing a fundamental information-theoretic understanding of quantum secure communication and devising practical and scalable implementations of quantum key distribution protocols in a photonic integrated chip platform.

I. OVERVIEW

The goal of this program is to experimentally and theoretically investigate the fundamental information capacity of optical communications and to develop revolutionary technology that will enable unprecedented information content, in excess of 10 bits per photon (bpp), while guaranteeing absolute security at high communication rates of 1 Gbps or more. The following sections detail the progress towards theoretical and experimental goals.

II. INFORMATION CAPACITY OF A PHOTON AND TRANSMISSION IN FREE SPACE

Three lines of work have been pursued during this reporting period. First, the theory of secrecy capacity for multiple-input, multiple-output, multiple-eavesdropper (MIMOME) classical channels with additive Gaussian noise is being extended to MIMOME bosonic channels. Whereas the classical case is characterized by Alice-to-Bob (transmitter to intended receiver) and Alice-to-Eve (transmitter to eavesdropper) channel matrices, the bosonic case requires a unitary transformation that couples the spatial modes controlled by Alice and a set of auxiliary (vacuum-state) spatial modes to the spatial modes observed by Bob and Eve. When Alice uses coherent-state encoding and both Bob and Eve employ heterodyne detection, the bosonic case reduces to the classical case in which the classical Alice-to-Bob and Alice-to-Eve channel matrices are sub-matrices of the overall unitary transformation. We have recently shown that the privacy capacity when Alice uses coherent-state encoding and Bob and Eve use optimum quantum receivers is given by replacing the classical Shannon information with the appropriate Holevo information. However, it remains to be seen whether coherent-state encoding is optimal. Toward this end we have conjectured that coherent-state encoding is optimal, and will be pursuing a proof that this is so. We expect that such a proof may rely on the as-yet unproven Entropy Photon-Number Inequality, whose proof would settle several other open classical-information capacities for bosonic channels.

The second theory area we are working is the quantum bootstrap protocol for secure communication. During the reporting period we have converted the abstract description of this protocol – which, in essence is a key expansion technique – into one that can be implemented with coherent-state (laser) light, phase shifters, and beam splitters. This linear optics setup has the advantage of being readily implemented and being robust to propagation loss and noise. The key step that remains is to evaluate the security of this system.

The last theory area we have been addressing is to determine and compare the cross-talk characteristics of multiple-spatial mode systems that use Hermite-Gaussian (HG) or Laguerre-Gaussian (LG) field patterns when propagation is through atmospheric turbulence. In the absence of turbulence, these two mode sets provide fully equivalent singular-value decompositions for propagation between Gaussian-attenuation soft apertures. In the presence of turbulence, however, that will no longer be the case, i.e., there will, in general, be cross talk between the fields collected at the receiver from different LG (or different HG) modes. We have established the general cross-talk evaluation setup for receivers that do not or do use adaptive optics. What remains to be done is numerical evaluation of the cross-talk integrals for these cases. The results of these evaluations will settle an important question regarding turbulence robustness. In particular, it has been hypothesized that LG modes will be more robust to turbulence than HG modes, owing to LG modes' carrying orbital angular momentum. We suspect that this may only be the case for LG modes

with different azimuthal indices, i.e., different orbital angular momenta.

Our effort is now picking up as a new postdoc, Ligong Wang, has arrived at MIT to begin work on the InPho projects. Ligong will be 50% time on the present program and 50% time on the PIECOMM program (the BBN-led InPho Classical Communication program).

III. PHOTONIC INTEGRATED CHIP

The experimental component of this project focuses on the development of an integrated photonic architecture for high-speed, photon-efficient quantum key distribution.

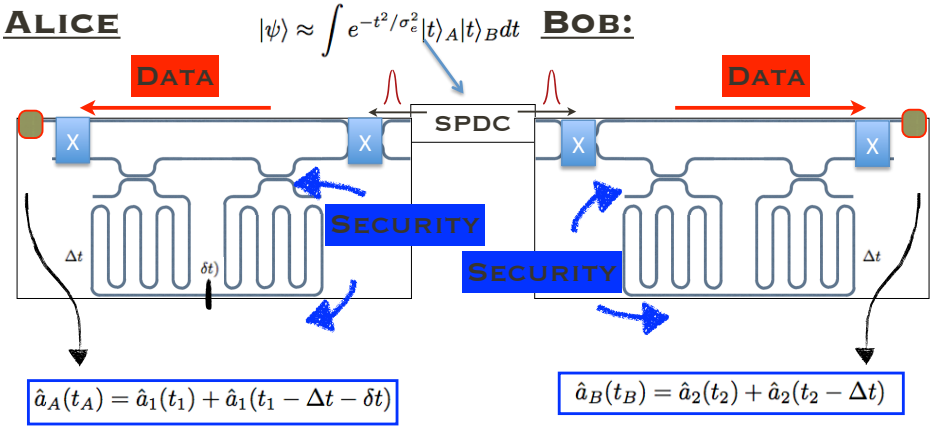

FIG. 1: An entangled photon state is generated by spontaneous parametric down conversion; this is approximated at the biphoton given in the top of the figure. One photon is sent to Alice, the other to Bob. These parties either measure the timing of the photon pair to establish a private key, or they check the security of the protocol using a Franson interferometer. The Franson interferometer employs two unbalanced MZ interferometers with time-difference Δt, enabling coherence measurements to $2\Delta t$. A small path difference δt is used to change the coincidence probability from maximum to minimum.

In the first phase, the chip will implement the QKD protocol using time-energy entangled photon pairs, which are generated using a spontaneous parametric downconversion (SPDC) source, as discussed in Sect. IV. Alice and Bob have identical chips which contain a photonic integrated circuit (PIC) for the key generation and the security check. An incident photon on Alice's or Bob's setup is analyzed either (1) directly on a photon detector or (2) after a Mach Zehnder interferometers that makes up one half of a Franson interferometer, which enables a measurement of the degree of entanglement between the two photons [1]. These measurements corresponds to projections in two bases, (1) and (2). A measurement by Alice reduces the entanglement, which could be detected in the Franson fringe visibility [2]. The optical circuit that implements these measurements is illustrated in Figure 1, in which the 'X' symbols represent switches that randomly channel photons between 'key generation' and 'security check' (the two switches in Bob's or Alice's setup are synchronized.) The probabilities of performing measurements in the 'key generation' or 'security check' bases can be adjusted dynamically to rapidly adjust the network performance to potentially changing conditions.

Several versions of different PIC designs were fabricated by us and our collaborators, using a combination of electron beam lithography and dry etching, and UV lithography for polymer couplers. The network contains the following essential components:

1. Inverse tapered polymer input/output couplers to/from Si waveguides. The measured loss is approximately 2-3 dB on each coupler, which satisfies the year-1 target. We are working to reduce the loss to $\sim$ 0.5-1.5 dB per coupler (the lower figure may be attained using directional fiber taper couplers currently under development).

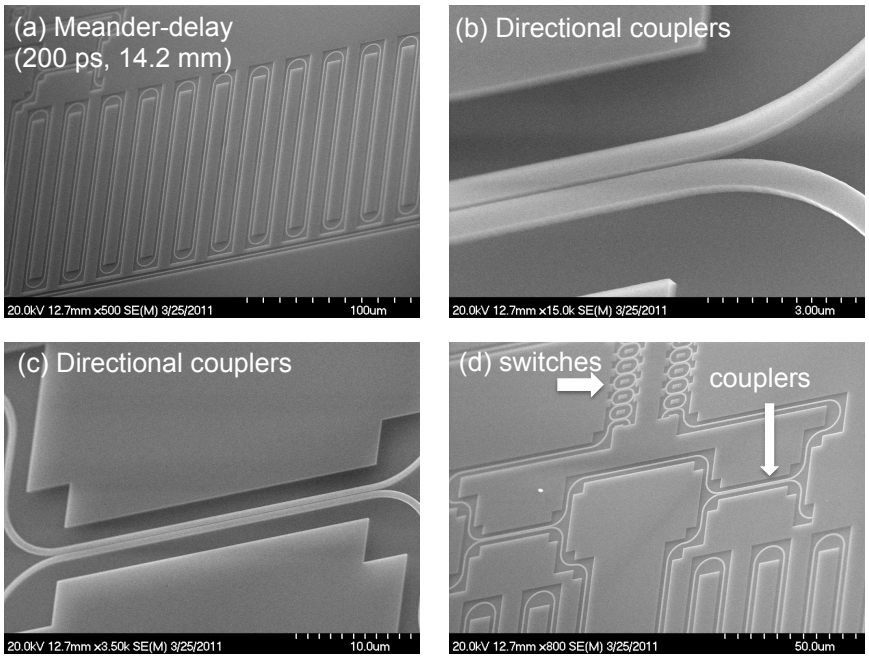

FIG. 2: Optical components of the first-generation photonic integrated chip for the time-energy entangled photon QKD.

2. Waveguides in silicon, as shown in Fig. 2. We have measured approximately 3 dB/cm loss in the standard single-mode ridge waveguides (left panel of Fig. 3). Here, the loss is dominated by scattering due to edge roughness (bulk silicon has loss below 0.01 dB/cm at 1500 nm). We are also implementing shallow, 'weak-confinement' waveguides that will be used for the delays in the unbalanced Franson in interferometer (right panel in Fig. 3). The loss for such waveguides can be as low as 0.1-0.3 dB/cm [3]. Based on these loss figures, we target, in Year 1, a Franson interferometer delay of 200 ps, sufficient for checking security for 400-ps period in QKD protocol. In Year 3, we target 0.1-0.2 dB/cm to achieve 5 ns delay and 8 bpp. Total loss in the Franson interferometer is then less than $\sim$ 10 dB.
3. Photonic switches to dynamically optimize the QKD protocol and to reduce, by a factor of two, the number of detectors used for security check and key-generation. The insertion loss can be less than 0.1 dB. We have implemented five cascaded ring resonators to construct a drop-filter with a top-hat spectrum instead of the typical Lorentzian spectrum [4]. The fabricated device is shown in Fig. 2(d). Such a resonator can be less sensitive to temperature fluctuations and allows for tighter spacing of wavelength channels in dense wavelength division multiplexing. However, we found that this filter design is difficult to fabricate and thus lossy; we will therefore adopt less demanding 1- and 2-ring drop filters.
4. Swap Gate: needed to generate polarization-path hyperentanglement from the output of the PPKTP waveguide; also needed to check security in the polarization and spatial degrees of freedom. This component is described in more detail in Sect. III A.
5. Multiplexing is used to scale up data rate beyond 10 bpp. Currently, our chips contain 1-4 wavelength channels. We are developing a special cascaded multiplexer/demultiplexer that has lower loss than standard systems as the number of drop ports scales logarithmically with the number of wavelength channels. In Phase III, we target 20 wavelength channels, each running at 8-9 bpp in time-energy basis, in addition to one spatial bit and one polarization bit. To avoid the need for 20 MZ interferometers, multiple wavelengths will be run simultaneously in one MZ interferometer, choosing wavelength spacings so that the same phase difference $\Delta\phi$ translates all wavelength channels between minimum and maximum interference.
6. Detector: we are developing a waveguide-integrated superconducting detector that will be integrated on the PIC, using a novel micro flip-chip bonding process. This is discussed in Section V. In future versions, photon

avalanche diodes may also be integrated directly on the PIC.

Optical measurements of the first-generation chip revealed several problems due to fabrication and mask imperfections. The mask imperfections were traced back to two problems which are shown in Fig. 5: an imperfect 'trench' layer near the drop-filters (left sub-figure), as well as a notch in the polymer mask (right sub-figure). We have addressed these problems in the meantime.

A. Swap-gate

Following from discussions with MIT and DARPA, it was highlighted that in the chip-scale implementation, it is easily possible to examine the entanglement quality between the spatial modes, in contrast to free-space entangled implementations. We think it is possible to extend to several spatial modes (in this case, perhaps in the which-path methodology) especially in the chip-scale implementation. Furthermore, the monolithic semiconductor approach is also intrinsically stable in each of these spatial modes, in contrast to free-space interferometers.

In the chip-scale approach, the spatial mode degree-of-freedom (DoF) might actually be preferable over polarization mode DoF. We note that this is because of possible typical polarization mode scrambling or rotation in the waveguides — in contrast to a distinct top or bottom path — although unintended polarization mode mixing can likely be suppressed by careful design of the waveguides.

At the detectors, it is simpler to measure in the polarization DoF. The SWAP gate converts the spatial mode entanglement into the polarization DoF for measurement. In this approach we can also check the entanglement visibility in each of the DoFs: time, spatial and polarization. The first-iteration InPho component chip is fabricated and under measurements in this quarter. The detected coincidence rate of the photon pairs had been improved up to $\sim 3,000$ pairs per second, in the infrared. Efficient on/off chip coupling has also been demonstrated with $\sim$ 10-dB total fiber-chip-fiber. In this quarter we have also examined the possibility for zero-phase accumulation in photonic delay lines. The second-iteration InPho layout design has been completed and taped out, and we plan to receive them in June.

In the next quarter, we seek to demonstrate entanglement on-chip and initial swap operation. Complete laser characterization of the photonic chip will also be completed. In the next quarter, we will start integration with the Franson interferometer as well as the switching capabilities, and possible fiber array coupling. In addition we can examine, theoretically and experimentally, the possibilities of (permutation asymmetric) entanglement across different DoFs.

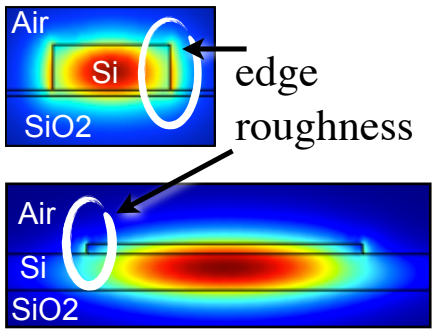

FIG. 3: Top: the standard ridge waveguide is 450 nm wide and 260 nm tall, but has high losses because of strong mode overlap with edge roughness. Bottom: the weakly confined mode has much smaller mode overlap with surface roughness and much lower losses are possible.

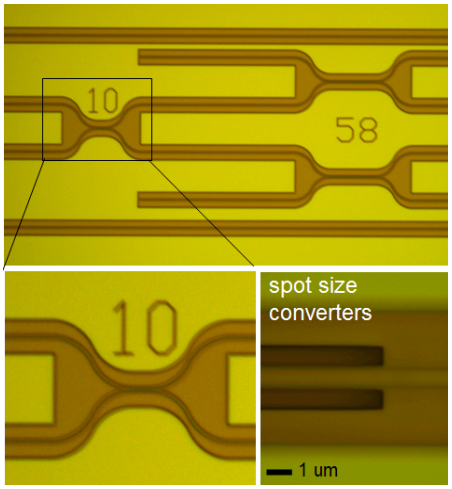

FIG. 4: Designed and fabricated first-iteration photonic chip for entangled photons. Low-loss couplers through spot size converters are included.

B. Milestones

Summary of major achievements in the PIC development:

- First-generation PIC fabricated

- PIC test-setup completed, including installation of scannable narrow-band laser and pulsed Ti:Sapph laser for switching.
- Constructed of setup for spontaneous parametric down conversion
- Ordered custom components for InGaAs avalanche detectors for single - photon IR detection (temporary solution before SNSPDs are ready).
- Demonstrated efficient on/off chip coupling using computer-controlled piezo actuators.
- Characterized chip using laser source.
- Completed design and fabrication of first-iteration InPho swap-gate component chip
- Demonstrated and improved coincidence rate of near-infrared photon pairs up to $\sim$ 3,000 detected pairs per second.
- Efficient on/off chip coupling with $\sim$ 10-dB total fiber-chip-fiber.
- Second-iteration InPho chip designed and under cleanroom fabrication.

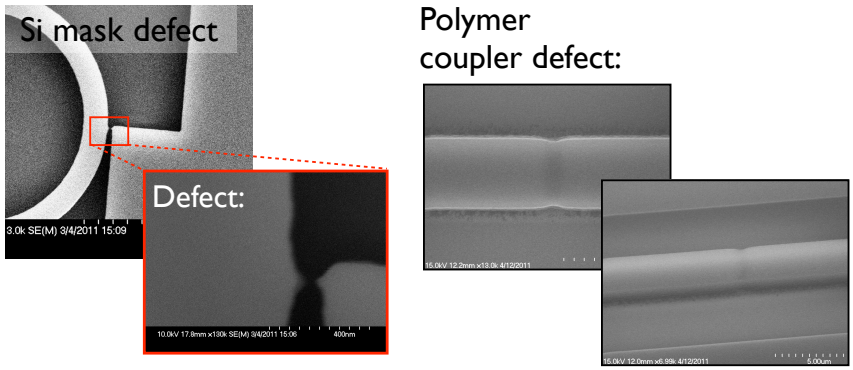

FIG. 5: Defects in the first-generation chip design. Left: electron beam lithography mask defect. Right: UV optical mask defect.

PIC development plan for the next 6 months:

- Complete full evaluation of chip with 200 ps delays (for 3-4bpp) with laser light: determine all losses, switching speed, isolation; estimate classical bit error rate using pseudorandom number generator. In particular, characterize all components:
  - Isolated straight waveguides of 4-5 different lengths
  - Isolated 50/50 directional couplers (2 input, 2 output)
  - Mach-Zehnders (2 input, 2 output)
  - Isolated massively unbalanced Mach-Zehnder
  - Franson interferometer
  - QKD without WDM
  - Single ring coupled to waveguide (many different radii, if possible)
  - Isolated ring filters (1 or 2, not 5)
  - Isolated linear WDM (serial filter array on waveguide)
  - QKD with WDM (two channels, serial WDM)
- Test PIC at single photon level

- Work with MIT on security analysis, including free space propagation, multiple spatial modes, privacy amplification
- Integrate SNSPD detectors onto Si PIC
- Entanglement measure with Franson interferometers
- Complete Fiber Array adaptation and testing (4 input, 4 output fibers)

IV. MIT ENTANGLED-PHOTON SOURCE DEVELOPMENT & TIME-ENERGY ENTANGLEMENT d-DIMENSIONAL QKD

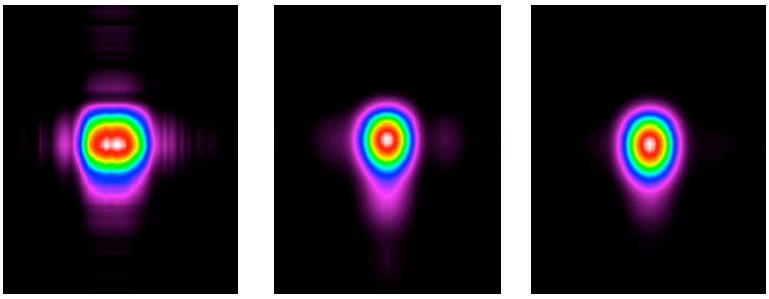

FIG. 6: Measured output mode for pump (left), signal (center), and idler (right).

A. Source development

We have tested the AdvR PPKTP waveguide and measured a downconversion generation efficiency of $\sim 2 \times 10^7$ pairs/s/mW of pump. For high entanglement quality, it is desirable to have no more than 4% probability of a pair within the measurement time interval of 40 ps that is limited by the expected SNSPD jitter, or about an average of 10^9 pairs/s that can be obtained with a pump power of 50 mW. Using single-mode laser inputs at the pump (780 nm) and output (1560 nm) wavelengths we evaluated the spatial mode outputs of the waveguide, as shown in Fig. 6. We have achieved excellent waveguide-to-fiber coupling efficiency of 75%, 77%, and 80% for pump, signal, and idler, respectively. Signal and idler fields have the same wavelength of 1560 nm but are orthogonally polarized. In the next 6 months, we will be making coincidence measurements of the downconverted light and setting up a Franson interferometer for testing 2-bit time-energy entanglement.

An important consideration relates to the generation of photon pairs at multiple frequency bands for wavelength division multiplexing. This can be accomplished either by employing degenerate photon pair generation with multiple laser fields or by using non-degenerate daughter photons at $\omega_{\text{pump}}/2 \pm \Delta\omega$. In the latter case, multiple wavelength bands can be excited using a single pump laser, which represents the practical choice.

B. InGaAs detectors

For initial testing of our sources, it is essential to have detectors that can handle high detection rate at telecom wavelengths. To this end, we have been working with NIST to assemble 4 self-differencing InGaAs APD single-photon counters based on a NIST-modified design of Andrew Shields that can achieve high detection rate of over 1 GHz. The InGaAs detectors and most of the electronics components have been purchased and received and ready for assembly. We have planned on an early May visit to NIST by graduate student Tian Zhong to learn the assembly and testing techniques. We expect to have 2 functional detectors by June.

C. Milestones

Achievements:

- Down-selection of nonlinear crystal: PPKTP is chosen for its orthogonally polarized outputs that allow simple implementation of polarization entanglement.
- PPKTP waveguide generation efficiency: measured 2×10^7 pairs/s/mW of pump, which is 50× more efficient than bulk crystal sources. (Note: more careful measurements show a generation efficiency that is higher than that shown on the site-visit slides.)
- Waveguide-to-fiber coupling: achieved 80% coupling efficiency from the waveguide to a single-mode fiber, and vice versa. Waveguide mode output matches well with calculations.

Plans for next 6 months:

- Assemble 2 high-detection-rate InGaAs detectors
- Explore spatial mode structure of waveguide outputs for direct generation of spatially entangled photons
- Demonstrate high-quality polarization entanglement
- Demonstrate 2-bit time-energy entanglement

V. WAVEGUIDE-INTEGRATED SNSPD

Process development for the SNSPD-on-membrane fabrication: One of the components of the waveguide-integrated detector system is an SNSPD fabricated on a membrane. A $\sim$ 1μm-thick membrane can be integrated on a chip which includes waveguides, photonic structures or single-photon sources and is thus a very scalable solution. However, the fabrication of SNSPDs on membranes is challenging and has not been demonstrated by other groups so far. We have evaluated several fabrication approaches so far. The current process is sketched in Figure 7. The SNSPDs are fabricated on a bulk SiN-on-Si substrate. The thickness of the Silicon nitride is on the order of $\sim$ 1μm. On top of SiN we grow a layer of NbN; we succeeded to control the deposition process, growing a $\sim$4 nm thick layer. The samples created are being used for process development which will lead to the devices fabrication. After the fabrication of the SNSPD, small slits (Figure 7) around the detector area are etched through the nitride layer via RIE. The chip is then dipped into KOH, which selectively etches the Silicon but not Silicon nitride. This wet-etch process undercuts the thin SiN layer with the detector on top. This small under-cut region can be easily released from the rest of the chip using microscopic probes.

Optical and electrical packaging for dip-probe setup: The waveguide (WG) integrated SNSPD will be tested in a dip probe setup, immersed in a liquid He bath ($T = 4.2$ K). For the characterization the dip probe needs packaging able to exchange optical and electrical signals between the room temperature setup and the cryogenic bath. For the optical part we are going to use a tapered single-mode optical fiber. This will be coupled at room temperature to the waveguide, as shown in Fig. 8. Once the alignment is performed we are going to maintain it by gluing the fiber and waveguide with a UV curable glue.

For the electrical packaging we designed a new structure to house the SNSPD chip inside of the probe head. The structure consists of three circular printed circuit boards that mate via surface mount ultra miniature coaxial (UMC) connectors. The SNSPD chip is clamped to the topmost PCB where wire bonds are made from the devices to 50 Ohm co-planar waveguides (used throughout). This board connects to a multiplexer PCB whose mating connectors are arranged so that half of the devices can be biased and read-out at one time, depending on the angle at which the multiplexer is connected to the SNSPD board. The opposite side of the multiplexer is mated to the 'Base board' PCB which connects the selected SNSPDs to cryogenic coaxial cables that run up the stem of the probe and terminate on SMA connectors at 300 K. Using this structure we can test up to 10 SNSPDs at once.

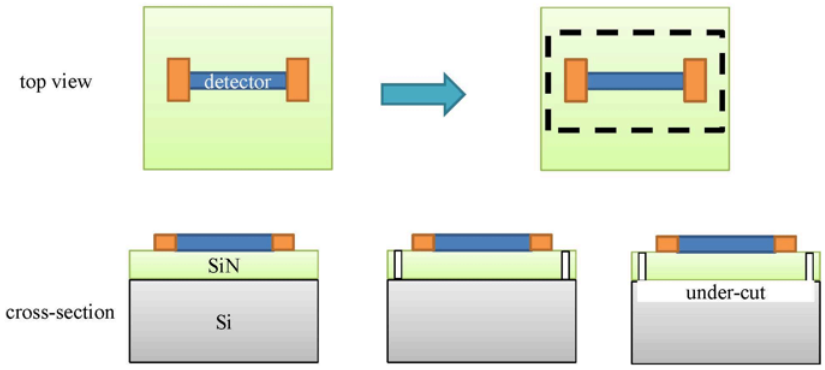

FIG. 7: Fabrication process for SNSPD on a membrane.

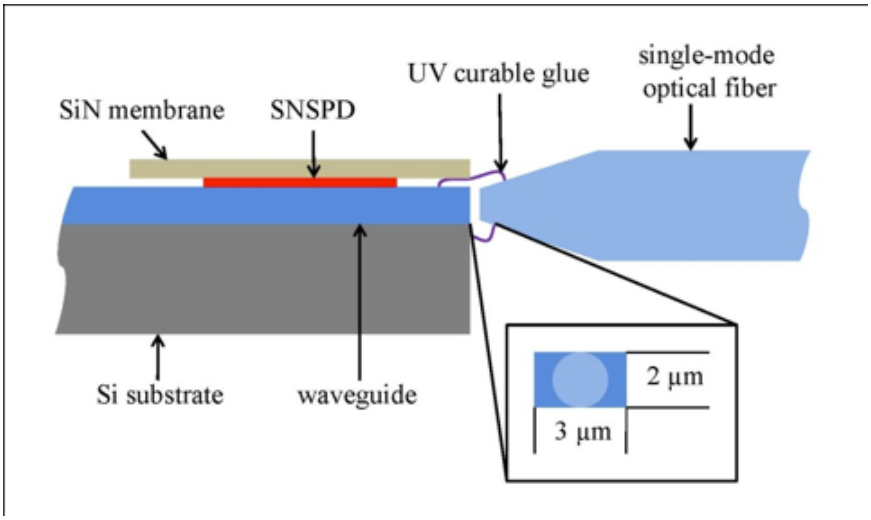

FIG. 8: **Single-mode optical fiber aligned to tapered waveguide**. The waveguide and the optical fiber are held together by a UV cured glue. Inset. Zoom of the waveguide coupling region cross-section (dark blue); the tip of the optical fiber (light blue) has to be as big as the waveguide coupling region.

[1] J. D. Franson. Two-photon interferometry over large distances. *Phys. Rev. A*, 44(7):4552–4555, Oct 1991.

[2] Irfan Ali-Khan, Curtis J. Broadbent, and John C. Howell. Large-alphabet quantum key distribution using energy-time entangled bipartite states. *Phys. Rev. Lett.*, 98(6):060503, Feb 2007.

[3] Po Dong, Wei Qian, Shirong Liao, Hong Liang, Cheng-Chih Kung, Ning-Ning Feng, Roshanak Shafiiha, Joan Fong, Dazeng Feng, Ashok V. Krishnamoorthy, and Mehdi Asghari. Low loss shallow-ridge silicon waveguides. *Opt. Express*, 18(14):14474–14479, Jul 2010.

[4] Yurii Vlasov, William M. J. Green, and Fengnian Xia. High-throughput silicon nanophotonic wavelength-insensitive switch for on-chip optical networks. *Nat. Photon*, 2:242 – 246, 2008.